CLAIMS

1. A communication device comprising:

an executing means for executing software;

a permission data storing means for storing permission data indicating permissible behavior for an application, which is a group of functions provided by execution of the software;

a checking means for checking, by accessing an external device before the software is executed, whether the permission data are valid; and

an execution control means for permitting said executing means to execute the software when, on the basis of a result of the check carried out by said checking means, the permission data are determined to be valid, and for not permitting said executing means to execute the software when, on the basis of the result of the check executed by said checking means, the permission data are determined to be invalid.

2. A communication device according to claim 1, wherein,

said communication device further comprises a determining means for determining whether it is necessary to carry out the check by said checking means, said determining means either carrying out or not carrying out the check on the basis of a determination made by said determination means.

3. A communication device according to claim 2, wherein,

said determining means comprises:

a counting means for counting a number of executions of the software; and

a frequency data storing means for storing frequency data indicating how frequently it is necessary to carry out the check; and wherein,

said determining means determines, on the basis of a number of executions of the software, as counted by said counting means, and on the basis of the frequency data stored in said frequency data storing means, whether it is necessary to carry out a check by said checking means.

4. A communication device according to claim 2, wherein,

said determining means comprises:

a timer means for providing time data indicating a present time; and

a time interval data storing means for storing time interval data indicating a time interval at which it is necessary to carry out the check; and

wherein,

said determining means calculates, on the basis of time data provided by said timer, a time period between a present time and a time recorded at a most recent execution of the software, and determines whether it is necessary to carry out the check by said checking means on the basis of the calculated time period and the time interval data stored in said time interval data storing means.

5. A communication device according to claim 1, wherein:

said communication device further comprises count data storing means for storing count data indicating a count of times that the software is allowed to be executed in a condition that said checking means is unable to make the check; and

said execution control means permits said executing means to execute the software in a condition that said checking means is unable to make the check up to a number of times which is indicated by the count data stored in said count data storing means.

6. A communication device according to claim 1 further comprising:

an updating means for obtaining update data from said external device, and updating the permission data stored in said permission data storing means on the basis of the update data.

7. A communication device according to claim 6, wherein:

said updating means

transmits, to said external device, update timing data indicating a timing of a most recent update of the permission data stored in said permission data storing means, when said checking means makes the check;

receives update data transmitted from said external device in response to the transmission of the update timing data; and

updates the permission data stored in said permission data storing means on the basis of the update data.

8. A communication device according to claim 1 further comprising:

a terminating means for instructing said executing means to terminate execution of the software when the application attempts to conduct behavior which the application is not permitted to conduct.

9. A communication device according to claim 1, wherein:

the permission data contain information on usage of at least one of an internal hardware resource of said communication device, an external hardware resource of said communication device, a software resource and a communication network resource.

10. A method for controlling a communication device comprising:

a step for transmitting to said communication device permission data, which indicates permissible behavior for an application, which is a group of functions provided by execution of software in said communication device;

a step for checking, by communicating data between said communication device and an external device, whether the permission data are valid, before the software is executed in said communication device; and

a step for permitting the software to be executed only when the permission data are determined to be valid on the basis of a result of the check.

11. A program for instructing a computer to execute:

a process for storing, in a storing means, permission data indicating permissible behavior for an application, which is a group of functions provided by execution of software;

a process for checking, by accessing an external device, whether the permission data are valid, before the software is executed; and

a process for permitting the software to be executed only when the permission data are determined to be valid on the basis of a result of the check.

12. A communication method comprising:

a step for transmitting from a communication system comprising

(a) a software data providing server device which stores software data containing software for providing a group of functions forming an application,

(b) a management server device which stores security descriptor data containing permission data indicating permissible behavior for the application, and

(c) an application descriptor data providing server device which stores application descriptor data indicating a storage location of the software data and a storage location of the security descriptor data,

to said communication device the application descriptor data;

a step for transmitting the application descriptor data from said communication system to said communication device;

a step for transmitting data indicating the storage location of the security descriptor data contained in the application descriptor data from said communication device to said communication system;

a step for transmitting the security descriptor data from said communication system to said communication device on the basis of the data indicating the storage location of the security descriptor data;

a step for storing the security descriptor data in said communication device;

a step for transmitting data indicating the storage location of the software data contained in the security descriptor data from said communication device to said communication system;

a step for transmitting the software data from said communication system to said communication device on the basis of the data indicating the storage location of the software data;

a step for installing, in said communication device, the software contained in the software data transmitted from said communication system to said communication device;

a step for checking, by communicating data between said communication device and said communication system before the software is executed in said communication device, whether the security descriptor data stored in said communication device are valid; and

a step for permitting said software to be executed in said communication device only when the security descriptor data are determined to be valid on the basis of a result of the check.